Restrictive Deterrence: Impact of Warning Banner Messages on Repeated Low-trust Software Use

Mario Silic[1,2,3], Dario Silic[2] and Goran Oblakovic[2]
[1]*University of St Gallen, St Gallen, Switzerland*
[2]*Zagreb School of Economics and Management, Zagreb, Croatia*
[3]*Luxembourgh School of Business, Luxembourgh, Luxembourgh*

Keywords: Fear Appeals, Software, Compliance, Warning Banner, Deterrence.

Abstract: This research paper focuses on the warning messages that are one of the last lines of defense against cybercriminals. The effectiveness of warnings in influencing users' behavior when using low-trust (potentially malicious) software has not been adequately addressed by the prior research. Using the restrictive deterrence theory, supported by the Communication-Human Information Processing (C-HIP) Model, we conducted an experimental study investigating the influence of warning messages on the repeated use of low-trust software. The results suggest that the use of low-trust software could be reduced in frequency, or completely abandoned, in the presence of warning messages, whereby security incidents could be better mitigated and reduced. We suggest several implications for practitioners and offer some interesting theoretical insights.

1 INTRODUCTION

Warnings or deterrent messages are a form of communication intended to inform users about the potential harm or risk they may incur (Wogalter, 2006c). For instance, tobacco manufacturers inform consumers about the health risks associated with smoking. However, quite often, the warnings are either ignored or have the opposite (i.e. boomerang) effect to that of the suggested behavior change (Bushman, 2006). In the computer world, this is partly explained by the fact that people do not read warnings (Egilman and Bohme, 2006) for the simple reason that people become habituated to them. In a recent study of user decisions ahead of the 'SSL warning' risk, it was found that over 70% of users continued through Google Chrome's SSL warnings but only 33% of users clicked through Mozilla Firefox's SSL warnings (Akhawe and Felt, 2013). This clearly indicates that the attention paid to warnings is very dependent on user experience and as such may lead to different behaviors. This user experience could be attributed to a simple design issue as warnings can take different forms (i.e. color, font, etc.) or different deterrent messages (i.e. content), which may impact the user's final decision. Other reasons suggested by the previous research relate to a lack of technical skills and general knowledge about the computer system (Sheng *et al.*, 2009) so that users often do not understand what 'SSL' or similar technological terms really mean and, consequently, do not pay attention to the displayed warning. Another reason that is advanced is the issue of trust in the computer system (Camp, 2006), as users may be easily tricked, for example, by phishing websites, without realizing that something is wrong.

Finally, no matter how effective, well-designed or appealing the warning message is, the decision will always be made by the end user. This is the whole purpose of having a warning message. The nature of the end user's decision will depend on many different factors. Some of these factors are inherent to the user him/herself, while some are more related to the warning message (Silic *et al.*, 2015). To better understand this interaction, the human-in-the-loop (HITL) framework was proposed as a general model to explain the interaction between the human and the computer system by suggesting a systematic approach to identify the potential causes of human failure (Cranor, 2008). The model is based on the Communication-Human Information Processing (CHIP) model that describes the processing steps undertaken by the user when confronted by the warning message (Wogalter, 2006b).

Silic, M., Silic, D. and Oblakovic, G.
Restrictive Deterrence: Impact of Warning Banner Messages on Repeated Low-trust Software Use.
In *Proceedings of the 18th International Conference on Enterprise Information Systems (ICEIS 2016) - Volume 2*, pages 435-442
ISBN: 978-989-758-187-8

Research into warning messages has shown that successful communication about the risks and benefits to users is possible, but only if the appropriate design is built, taking into account initial beliefs, message content and modality (Andrews, 2011). This communication can be influenced by the restrictive deterrence theory, which suggests that the frequency of repeated actions will decrease in the presence of sanctions (Gibbs, 1975). Hence, according to the C-HIP model, it is expected that the user will stop his/her activities if he or she pays attention to the warning message. Furthermore, despite the fact that most of the research has focused on the effectiveness of warnings in preventing the occurrence of a risky event, no studies have investigated the effect of warning banner messages on the progression and duration of the user behavior. Specifically, no prior study has examined the relationship between warning messages and low-trust (i.e. potentially malicious) software. Low-trust software is any software for which the source cannot be easily identified (e.g. software posted by an anonymous programmer on sourceforge.org repository) (Silic, 2013; Silic and Back, 2015). Such software can be malicious and can jeopardize users' privacy (e.g. by stealing private information). Hence, relying on the restrictive deterrence and supported by the Communication-Human Information Processing (C-HIP) model, we explore the impact of warning messages on the duration and progression of low-trust software use by measuring user behaviors and decisions. Next, we describe our theoretical background, after which we present the results, followed by the discussion and finally, the conclusions.

2 THEORETICAL BACKGROUND

2.1 Communication-Human Information Processing (C-HIP) Model

Research into warning messages has been categorized into the Communication-Human Information Processing (C-HIP) model (Conzola and Wogalter, 2001; Wogalter, 2006a). The C-HIP model posits that in order to communicate the warning (message), several factors have to be considered: the source, the channel, and multiple aspects of the receiver. The entire communication process starts with attention and is followed by comprehension, attitudes, beliefs and motivation. The source of the warning message transmits the presence of a certain hazard through a channel (Chen *et al.*, 2014). It might be that users do not pay attention to icons that represent SSL warnings (Grier *et al.*, 2008) because the channel (warning banner message) is either inefficient in transmitting the risk, or it might be that the user has necessary skills to understand the risky situation and simply ignores the warning. In this research, we focus on the channel and the attention aspects, which are one of the most important factors in shaping the user's behavior. The channel is the warning banner message that is displayed to users, informing them about the risks they may incur if they continue with their actions. For instance, if the user does not pay attention to the warning message then all the subsequent steps (e.g. comprehension) will be ineffective. The user's attention can often be gained through simple visual aspects (e.g. size, colors, graphics) (Laughery and Wogalter, 2006). Hence, for the communication to be attractive, a warning has to be conspicuous or salient relative to its context (Sanders and McCormick, 1987).

2.2 Restrictive Deterrence

Deterrence theory originates from the Criminology field and proposes that individuals who intend to commit a crime or an antisocial act can be dissuaded if sanctions and disincentives that are relevant to these acts are implemented (Straub and Welke, 1998). In the organizational context, if an employee violates information security policies, there is a high probability that he or she may be fired as a consequence of his or her acts. Overall, the deterrence theory posits that there is a high likelihood of being caught and punished severely. Recently, contemporary theoreticians proposed the 'restrictive deterrence' model which represents the process whereby offenders limit the frequency and severity of their individual offending (Gibbs, 1975; Jacobs, 2010). According to Gibbs (1975), restrictive deterrence is "the curtailment of a certain type of criminal activity by an individual during some period because in whole or in part the curtailment is perceived by the individual as reducing the risk that someone will be punished as a response to the activity" (1975: 33). Few studies have examined the restrictive deterrence aspect and its impact on deterring the user from committing risky or illegal actions (Maimon *et al.*, 2014). When it comes to the low-trust software context, the offender is the user him/herself. Indeed, the user has the choice, when confronted with the warning banner message, of

whether to continue or to stop his or her action. By continuing, the user makes a conscious decision, having been informed about the possible sanctions that he or she may incur. However, this is true only if the user has paid attention to the context displayed by the warning message. In such a case, according to the restrictive deterrence theory, it is expected that the user will reduce the frequency of his/her acts as the user will be sanctioned at some point in time.

Past studies have investigated the restrictive deterrent concept mostly through qualitative research methods (e.g. Jacobs, 1996; Jacobs, 2010; Gallupe *et al.*, 2011; Jacobs and Cherbonneau, 2014), investigating relatively small samples (e.g. Beauregard and Bouchard, 2010). One important reason for this lack of quantitative studies could be access to data, as not only is it difficult to conduct a study that deals with the malware context, but there is also the problem of how to avoid bias by not recruiting participants directly. Overall, empirical investigations into the restrictive deterrent concept are still relatively scarce.

2.3 Research Hypothesis

The main objective of the warning message is to capture users' attention and convey information about the possible hazard (Bravo-Lillo *et al.*, 2013). Consequently, according to C-HIP, in this communication delivery process, if a user's attention is switched to the warning message, we can expect to see increased compliance and better decision making. However, users tend to easily ignore the warnings. This is because they usually have more trust and confidence when using high-reputation websites (Sunshine *et al.*, 2009). This means that users may have higher levels of trust when downloading software from well-known and established websites such as sourceforge.org. In that context, users may pay less attention to the underlying risks and may be more willing to ignore possible risk consequences. Hence, supported by the restrictive deterrence model (Gibbs, 1975), we argue that when the user is repeatedly using the software, the user may pay more attention to a warning message that is displayed to inform him/her about a possible hazard. Consequently, this may lead to decreased software use and, consequently, to abandonment. Therefore, we hypothesize that:

Repeated software use will decrease and will lead to abandonment in the presence of the warning banner message.

2.4 Study Methodology

2.4.1 Participants

We did not recruit any participants for the study, which increases the study's validity. In such a way, we were able to create and simulate a genuine environment. Institutional Review Board (IRB) approval was given to the data collection and human-subject protocols were followed. In addition, each participant had to provide his or her consent to taking part in a research study. Once the application was started, a dialog box opened, informing the user about the study's objectives (and informing them that no identifiable information would be collected) as well as asking them to confirm their participation. If users chose not to participate, then we did not measure any of their activities (this was set programmatically). Hence, users were fully aware of the experiment. Also, all participants had to accept the end user license agreement (EULA) which, among other clauses, stipulated that "By downloading this software, you consent to send usage information for research purposes".

2.4.2 Research Design

We used the experiment method to explore and measure the progression, frequency, and duration (i.e. time) of user behavior when confronted by a warning banner message. The installation and consequent use of the software was operationalized as an event that had a certain duration (start and end). To measure and operationalize these events we created a randomized experiment using a VB.net application that was created to support our study. The application was fully functional software providing PDF manipulation possibilities to the end user. To conduct our study, we used the open-source software repository Sourceforge.org, where the final version of the application was published. Upon the launch of the application (a dialog box asking for the user's content appeared prior to the application launch), and after clicking on the 'START' button, the application randomly displayed either a control message or the warning banner message. Figure 1 shows the design of the warning message. For the warning message we used the McAfee warning design, which is one of the most commonly used forms of AntiVirus software and as such provided a genuine environment. Next, we measured the events, timing the start and the termination of each instance of software use. This allowed us to measure the event from its start (clicking on the 'START' button) till its end (clicking

on either the 'Exit' or 'Continue' button displayed in the warning message). This was operationalized by two dependent measures: *action cessation* (0 meant that the user had stopped the software use by clicking on Exit, while 1 indicated that the user had continued his/her software use, ignoring the warning message) and *action duration* represented a continuous measurement that counted the elapsed time (in milliseconds) between the start and the end of the event. The entire data collection process was fully anonymous and invisible to the user.

Figure 1: Different warning messages.

2.4.3 Method used for Analysis

To analyze the effects we used the Kaplan-Meier Survival Curve, which is an estimator used to estimate survival time from the lifetime data. It is very commonly used for medical purposes to estimate and measure the fraction of patients surviving after receiving treatment. The Kaplan-Meier Curve is a popular method when it comes to analyzing different survival times (times-to-event). Overall, the Kaplan-Meier method is a nonparametric method used to estimate the probability of survival past given time points (i.e. it calculates a survival distribution) (Kaplan and Meier, 1958). Time to event represents an event course duration for each user, having a beginning and an end. In this type of analysis, each participant is characterized by three variables: 1) the duration; 2) the status at the end of the event (exit or continue); and 3) the warning type.

3 RESULTS

In total, 1250 events were recorded. In Table 1 a detailed overview of the warnings displayed and the corresponding user actions can be found. Exit action was chosen in 36% of all cases, while 64% of users decided to continue with the software use. When it comes to the warning types, as expected, for the 'No warning' message few users (10%) stopped using the application, while the vast majority (90%) continued. For the warning message, 63% of users found the message to be rather persuasive and thus, decided to exit the software use, compared to 37% of users who continued.

Table 1: Overview of display warnings and users' actions.

Warning type	Exit action (decision=0)	Continue action (decision=1)	Total
Warning	590 (63%)	348 (37%)	938
No Warning	31 (10%)	281 (90%)	312
Grand Total	621 (36%)	629 (64%)	1250

Furthermore, to understand whether warning messages influence the time until termination, we used the survival function – the Kaplan-Meier Survival Curve (Figure 2). The results of this analysis clearly show that across all event points in the presence of the warning message, the survival time is much shorter. Specifically, this means that in the presence of the warning message, the duration of the low-trust software use is very much shortened and the message leads to a faster use termination.

Having inspected the cumulative survival plot time, we made an initial assumption regarding how users behave when confronted with a warning banner message. In order to understand the typical time duration until users stop their software use, and consequently reduce the frequency, we will look at the means and the medians for survival times (Table 3). Table 3 displays the mean and median survival times, and associated statistics, for each of our intervention groups.

We can see from the results in Table 3 that the median survival time for the warning message is 5055 milliseconds with 95% confidence intervals from 3104.36 to 7005.640 milliseconds.

As the median is calculated as the time at which the cumulative survival proportion is 0.50 or less (i.e. 50% or less) for the warning message, this indicates that users need more time to make a decision and their decision making process is affected by the warning message content. Finally, in order to understand the differences between the first observed events (first software use) and all of the following software uses by the user, we used the Cox proportional-hazard regression model. The Cox model allows the investigation of the relationship between the survival of the event and independent measures (Box-Steffensmeier and Jones, 2004).

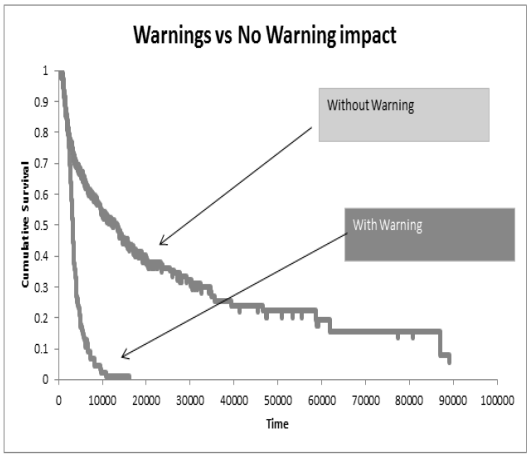

Figure 2: Kaplan-Meier Survival Curve: warning vs no warning impact.

In other words, it will provide evidence of whether the event duration, progression and repeated software use are decreased in the presence of the warning banner message.

The results, calculated using IBM SPSS software, are presented in Table 2. We can see that for the first observed events (first software use) the hazard ratio is 1.28 times lower than for the second observed event hazard ratio (second use). Also, the hazard ratio for the first observed events is more than 3 times greater than for all incidents. Clearly, this indicates that the hazard ratio estimate of the warning measure shows that the warning message significantly increases the rate of the second observed event compared to the first observed event. This leads to much shorter event duration and confirms that the frequency of the repeated software use is decreased in the presence of the warning banner message.

4 DISCUSSION

Our study aimed to answer the question of whether repeated software use would be decreased, leading to abandonment, in the presence of the warning banner message. By conducting an online experiment involving anonymous participants, we found that repeated software use will be decreased in the presence of the warning banner message.

To the best of our knowledge, this is one of the first studies that goes beyond the initial understanding of the user's binary decision making process (continue or exit), as we tried to understand whether the warning banner message has any effect on repeated software use. In other words, this study aimed to determine whether, ultimately, the warning

Table 2: Cox proportional hazards survival regression results.

	Coefficient (standard error)	**Hazard ratio**	**Log Likelihood**
First observed events (N=348)	0.75*	2.45	-170.11
Second observed events (N=235)	0.45*	3.15	-190.56
All observed events (N=1250)	0.181*	0.653	-1238.125
∗p < .05 (two-tailed);			

banner message, based on restrictive deterrence theoretical assumptions, leads to decreased software use and consequently to abandonment. Although prior research has produced often inconclusive and mixed results about the effectiveness of warning messages in deterring and preventing the occurrence of criminal incidents (e.g. it was found that warnings are effective in deterring some illegal behavior such as the claim padding of insured persons (Blais and Bacher, 2007) but ineffective in deterring prostitution (Lowman, 1992)), our study clearly shows that warning messages have a high impact on the user's decisions. Consequently, warning communication impacts the user's behavior. This is particular interesting as the human aspect was identified as being the weakest link in the entire information security ecosystem. In the current cybercrime era, a significant number of criminal acts are committed, facilitated or enabled (voluntarily or otherwise) thanks to the involvement of the human factor. It is evident that users will not cease their illegal behaviors in the near future as there will always be factors that will be either difficult to tackle (e.g. users' technological skills) or difficult to influence and change (e.g. human decision making).

However, a better understanding of how humans behave throughout the event duration may lead the way to a better understanding of the effectiveness of the existing measures. Clearly, our study shows that in the presence of the warning banner message user behaviors are influenced and changed.

4.1 Theoretical Implications

Our study offers some interesting theoretical implications. We used restrictive deterrence theory, supported by the C-HIP model, and found that restrictive deterrence can be rather efficient in

Table 3: Mean and median survival times.

Means and Medians for Survival Time

WARNING TYPE	Mean[a]				Median			
	Estimate	Std. Error	95% Confidence Interval		Estimate	Std. Error	95% Confidence Interval	
			Lower Bound	Upper Bound			Lower Bound	Upper Bound
No Warning	7111.4	2404.1	2399.3	11823.4	3282.0	153.0	2981.9	3582.0
Warning	18282.7	3509.5	11404.0	25161.4	5055.0	995.2	3104.3	7005.6
Overall	14896.1	2545.8	9906.3	19886.0	3382.0	250.7	2890.5	3873.4

a. Estimation is limited to the longest survival time if it is censored.

explaining the user's decision making process and the sanctions or hazards that the user may incur, in the case of non-compliance. This is an interesting insight as it provides some new directions for the research. Indeed, past studies have mostly focused on the binary decision making process and have tried to simply understand the 'yes' or 'no' without further understanding what happens if the user chooses yes – could there be any abandonment and if so, when does it occur? In this context, restrictive deterrence becomes particularly interesting. By applying it to our unique context, we see that the user's conscious decision making process is ultimately affected by the threat of sanctions, and the applying it to our unique context, we see that the user's conscious decision making process is frequency of repeated use is decreased.

4.2 Implications for Practice

This study raises some interesting implications. Firstly, we believe that the question of the human factor in the cybercrime area could be much better tackled if we design more convincing warnings about the risks that users may incur. We argue that most of the existing communication is rather inefficient as it mainly focuses on the legal or compliance aspects. Instead, communication that is built around the direct consequences for the user him/herself may prove to be much more effective and persuasive. In today's world users are constantly warned about risks and harm that may befall them, but this does not seem to be sufficiently effective. For instance, a recent study on the effect of warnings on decreasing cigarette smoking showed that the standard warning messages (e.g. smoking can kill you) are ineffective (Peters *et al.*, 2014). Instead, the study found that when smokers are informed of the fact that someone they care about may be seriously impacted by their smoking (e.g. the health of your children could be seriously impacted) a positive change in their behavior was observed with a much higher percentage of people stopping smoking. Hence, we recommend rethinking the way in which we communicate warnings to users when using software that has, by default, a lower reputation. One such example is when the user is installing an unverified driver, the Windows operating system displays a warning message informing the user that Windows cannot verify the publisher of the driver software. The displayed warning message proposes two options: 1) Not to install the driver and go to the manufacturer's website to check for the latest version of the driver; or 2) Install the driver – in this option the user is warned to install drivers only from verified sources as unverified software may harm their computer. However, we argue that this is a completely ineffective means of communicating the potential risk. Surely, for a user with advanced technical skills and knowledge, this warning message is probably sufficient, but that may not be the case for an average computer system user who is not even sure what a driver is or what kind of place and importance it has once installed in the heart of the operating system. Transforming the standard warning message to a warning message that highlights the risk in a much more direct way for the average user is not an easy task, as it would require a new design thinking approach that could be adaptable to various contexts. However, by following an approach whereby, instead of communicating the fact that 'Windows can't verify the publisher' we would for instance communicate the message that 'Installing this driver could DELETE all of your data and damage your hard disk', an existing vicious circle between the cybercriminals, the human factor and targets could be better addressed to decrease and mitigate the risk. Indeed, cybercriminals are exploiting the vulnerable human factor as people rely on technology to inform them and provide input for their decision making process when confronted by a risk situation in which they have to make a choice. Also, by increasing the quality of the input we communicate to the user through the warning, we would certainly decrease the number of potential targets for cybercriminals. This

communication enhancement could be applicable to almost any area. For example, in phishing attacks via email, the warning message could be displayed by the operating system when certain patterns are detected in the email content. Obviously, one drawback to this approach is that the number of warning messages could significantly increase, and finding the right balance could be another challenge to face. Ultimately, we do not want to sacrifice security to jeopardize the user's experience.

4.3 Limitations and Future Research

Our study has several limitations. Firstly, we were unable to identify the users who downloaded the application. This limits our findings as a better understanding of who they are, their technical skills, experience, etc. could bring more precision to the results. We suggest that future studies might incorporate this aspect and attempt to understand how people's background, cultural aspects, etc. affect their overall software use. Secondly, we used an online open-source repository to place our application. While many of these repositories are labeled as trusted, often they are limited to medium to advanced users, as novice users do not have sufficient technical skills to use these websites. This could have some limitations in terms of the results as it could be expected that novice users would be more inclined to abandon their software use immediately rather than continuing. Overall, we suggest that future studies should build on the restrictive deterrence theory and use the C-HIP model to further theorize how different aspects of the C-HIP model interact with the restrictive deterrence premises. It could be interesting, for instance, to understand how attention and comprehension are related to the frequency of repeated software use.

5 CONCLUSIONS

The effectiveness of warnings in influencing users' behaviors when using low-trust (potentially malicious) software has not been adequately addressed by prior research. This study represents a first attempt to illustrate the way in which warnings can reduce the frequency and the duration of low-trust software use. These results are particularly interesting for IT managers as they suggest that the use of non-approved software could be reduced in frequency, or completely abandoned, in the presence of warning messages, so that security incidents could be better mitigated and reduced.

REFERENCES

Akhawe, D. and Felt, A. P. (2013) *Usenix Security*.

Andrews, J. C. (2011) 'Warnings and disclosures', *Communicating Risks and Benefits: An Evidence-Based User's Guide*, pp. 149-61.

Beauregard, E. and Bouchard, M. (2010) 'Cleaning up your act: Forensic awareness as a detection avoidance strategy', *Journal of Criminal Justice*, 38(6), pp. 1160-1166.

Blais, E. and Bacher, J.-L. (2007) 'Situational deterrence and claim padding: Results from a randomized field experiment', *Journal of Experimental Criminology*, 3(4), pp. 337-352.

Box-Steffensmeier, J. M. and Jones, B. S. (2004) *Event history modeling: A guide for social scientists*. Cambridge University Press.

Bravo-Lillo, C., Cranor, L. F., Downs, J., Komanduri, S., Reeder, R. W., Schechter, S. and Sleeper, M. (2013) *SOUPS '13 Proceedings of the Ninth Symposium on Usable Privacy and Security*.

Bushman, B. J. (2006) 'Effects of warning and information labels on attraction to television violence in viewers of different ages', *Journal of Applied Social Psychology*, 36(9), pp. 2073-2078.

Camp, L. J. (2006) 'Mental models of privacy and security', *Available at SSRN 922735*.

Chen, T.-C., Stepan, T., Dick, S. and Miller, J. (2014) 'An anti-phishing system employing diffused information', *ACM Transactions on Information and System Security (TISSEC)*, 16(4), p. 16.

Conzola, V. C. and Wogalter, M. S. (2001) 'A Communication-Human Information Processing (C-HIP) approach to warning effectiveness in the workplace', *Journal of Risk Research*, 4(4), pp. 309-322.

Cranor, L. F. (2008) 'A Framework for Reasoning About the Human in the Loop', *UPSEC*, 8, pp. 1-15.

Egilman, D. and Bohme, S. (2006) 'A brief history of warnings', *Handbook of Warnings. Lawrence Erlbaum Associates, Mahwah, NJ*, pp. 35-48.

Gallupe, O., Bouchard, M. and Caulkins, J. P. (2011) 'No change is a good change? Restrictive deterrence in illegal drug markets', *Journal of Criminal Justice*, 39(1), pp. 81-89.

Gibbs, J. P. (1975) *Crime, punishment, and deterrence*. Elsevier New York.

Grier, C., Tang, S. and King, S. T. (2008) *Security and Privacy, 2008. SP 2008. IEEE Symposium on*. IEEE.

Jacobs, B. A. (1996) 'Crack dealers' apprehension avoidance techniques: A case of restrictive deterrence', *Justice Quarterly*, 13(3), pp. 359-381.

Jacobs, B. A. (2010) 'DETERRENCE AND DETERRABILITY*', *Criminology*, 48(2), pp. 417-441.

Jacobs, B. A. and Cherbonneau, M. (2014) 'Auto theft and restrictive deterrence', *Justice quarterly*, 31(2), pp. 344-367.

Kaplan, E. L. and Meier, P. (1958) 'Nonparametric estimation from incomplete observations', *Journal of*

the American statistical association, 53(282), pp. 457-481.

Laughery, K. R. and Wogalter, M. S. (2006) 'Designing effective warnings', *Reviews of human factors and ergonomics*, 2(1), pp. 241-271.

Lowman, J. (1992) 'STREET PROSTITUTION CONTROL Some Canadian Reflections on the Finsbury Park Experience', *British Journal of Criminology*, 32(1), pp. 1-17.

Maimon, D., Alper, M., Sobesto, B. and Cukier, M. (2014) 'Restrictive deterrent effects of a warning banner in an attacked computer system', *Criminology*, 52, pp. 33-59.

Peters, G. J. Y., Ruiter, R. A. and Kok, G. (2014) 'Threatening communication: A qualitative study of fear appeal effectiveness beliefs among intervention developers, policymakers, politicians, scientists, and advertising professionals', *International Journal of Psychology*, 49(2), pp. 71-79.

Sanders, M. S. and McCormick, E. J. (1987) *Human factors in engineering and design*. McGRAW-HILL book company.

Sheng, S., Wardman, B., Warner, G., Cranor, L., Hong, J. and Zhang, C. (2009) *Sixth Conference on Email and Anti-Spam (CEAS)*. California, USA.

Silic, M. (2013) 'Dual-use open source security software in organizations – Dilemma: Help or hinder?', *Computers & Security*, 39, Part B(0), pp. 386-395.

Silic, M. and Back, A. (2015) 'Identification and Importance of the Technological Risks of Open Source Software in the Enterprise Adoption Context'.

Silic, M., Barlow, J. and Ormond, D. (2015) 'Warning! A Comprehensive Model of the Effects of Digital Information Security Warning Messages', *The 2015 Dewald Roode Workshop on Information Systems Security Research, IFIP*. Dewald IFIP, pp. 1-32. doi: 10.13140/RG.2.1.2550.1202.

Straub, D. W. and Welke, R. J. (1998) 'Coping with systems risk: security planning models for management decision making', *Mis Quarterly*, pp. 441-469.

Sunshine, J., Egelman, S., Almuhimedi, H., Atri, N. and Cranor, L. F. (2009) *18th USENIX Security Symposium*.

Wogalter, M. S. (2006a) 'Communication-Human Information Processing (C-HIP) Model', in Wogalter, M. S. (ed.) *Handbook of Warnings*. Mahwah, NJ: Lawrence Erlbaum Associates, pp. 51-61.

Wogalter, M. S. (2006b) 'Communication-human information processing (C-HIP) model', *Handbook of warnings*, pp. 51-61.

Wogalter, M. S. (2006c) 'Purposes and scope of warnings', *Handbook of Warnings. Lawrence Erlbaum Associates, Mahwah, NJ*, pp. 3-9.